

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

Vol. 3, No. 9 | September 2003

Trends

Instant Messages Emerging as Newest Source of E-evidence

Instant messaging has thus far typically been the domain of 11- to 16-year-olds, their rapid-fire e-conversations consisting of sentence fragments and computer symbols unintelligible to most of the adult world. But now IM is entering the workplace, presenting both new discovery challenges and opportunities.

IM, which allows for “real-time” exchanges of text messages, mostly exists “under the radar” in workplaces, according to Michael R. Overly, special counsel to the Information Technology Department at the law firm Foley & Lardner in Los Angeles. “Employees are using this without their employer’s knowledge,” he said.

Overly explained that employees are installing IM software on their computers and “the employer has no idea they’re doing it.”

“Companies are getting very concerned,” he said.

While some employers remain unaware of IM, others are embracing the electronic communications option.

“In general, IM is becoming an acceptable corporate communication tool,” said Bob Chatham, principal analyst at Forrester Research, a Boston-based firm that identifies and analyzes technology trends and their impact on business.

IM is “in between e-mail and the phone,” Chatham said. “It’s certainly a convenient tool.”

However, the potential for abuse of the medium exists, he added. Workplace technology experts agree that IM presents employers with many of the same issues as e-mail: security of transmissions, diminished productivity, and liability for offensive messages.

“It raises all the issues that we’ve always seen with e-mail,” Overly said, only many of the problems are “heightened” because of the speed of IM. “We always refer to instant messaging as being e-mail on steroids,” he said.

Implications for Litigators

Nancy Flynn, co-author of *E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication*, published by AMACOM, observed that some analysts are predicting that in a few years, IM will overtake e-mail as the number one business electronic communication medium.

Jonathan A. Segal, an attorney with the Philadelphia-based firm of Wolf, Block, Schorr & Solis-Cohen, cautioned that one problem with IM is that employees are likely to be “transmitting messages before they think.”

As with e-mail, these instant messages can emerge as the smoking gun in discrimination and harassment actions.

“People don’t think about what

Inside

- | | |
|------------|--|
| 3 | Conference Report:
Agreements Should Govern Experts’ Work Product Disclosure, Panelists Urge |
| 4 | Talking Tech: Do-It-Yourself Electronic Discovery Tools |
| 6-9 | Cases: Copying In-house Counsel on E-mail Doesn’t Create Attorney-Client Privilege • Smith & Wesson E-mail No ‘Smoking Gun,’ Due to Attorney-Client Privilege • No ‘Work Product’ Protection For E-mail Prepared Prior to Decision to Represent |
| 9 | Point of View: Former Police Investigators Make Top-notch Computer Forensics Experts |
| 12 | Calendar |

they’re saying. It’s worse than e-mail in that regard,” Chatham said.

“It’s impulsive. It’s not great for sensitive or emotional issues,” Chatham said of IM. Workplace communications usually “should be a little more thoughtful.”

“With instant messaging, it’s literally like having a conversation because you’re typing in real time,” Overly said. Moreover, like e-mail, instant messages are recorded on a system, so messages do not just disappear when they are deleted. Overly is the author of *Document Retention in the Electronic Workplace*, a 2001 publication of Pike & Fischer, Inc.

continued on page 2

continued from page 1

According to Overly, most employees have come to understand the permanent nature of e-mail. However, he said, they still see instant messages as only existing for the duration of the electronic conversation. "People think of it as something that can be deleted immediately," Overly said.

Because of its conversational nature, instant messages can be perfect for attorneys looking for evidence of a company's wrongdoing.

Like e-mail, IM can "come back to haunt you in litigation," Flynn warned. And because IM is "just chat," she said, there is a greater likelihood of an offhand remark being sent that will offend someone and trigger a lawsuit.

Employees need to be made aware that instant messaging "creates a business record," Flynn said. This record is "essentially corporate DNA," she said. "If you get sued, this is the evidence."

Retaining IM Logs

Retaining logs of instant messages is "another big issue," Flynn said. She explained that in employment discrimi-

nation or harassment lawsuits, "you can bet e-mail and instant messages are going to be subpoenaed." If your client cannot produce the requested information, she said, "you are going to be penalized by the court."

Unfortunately, Flynn said, most IM systems also do not have built-in archiving systems.

Banks and securities firms must pay particular attention to e-mail and IM retention because of industry regulations specifying that they must maintain records of certain communications, Flynn noted.

According to Overly, a concern in the securities industry is that while firms are required to maintain records of electronic conversations, an employee with IM capabilities could be instant messaging with clients without the company even knowing about it. "You can see where there might be a problem," he said.

Guidance for Your Corporate Clients

In terms of monitoring, Flynn said that while the vast majority of employers now monitor their employees' e-mail, IM pre-

sents a challenge because of the various IM services used by workers. "You might have several dozen instant messaging devices at work, so how are you going to monitor them?" Flynn asked. Employers need to standardize their IM system and then put monitoring software in place, she said.

While most e-mail monitoring devices are fairly "mature," Overly said, with IM "it's a bit more difficult." He predicted that the evolution of monitoring software will involve techniques that cover both e-mail and instant messaging.

Unlike company e-mail accounts, employees' IM accounts are generally set up at home by employees, noted David Sobel, general counsel of the Electronic Privacy Information Center. As long their employer is silent on the matter, most employees will believe their IM use at work is a personal, private matter, Sobel said, although he noted that actual law in this area is uncharted.

The expectation of privacy by employees in such a case may be reasonable, Sobel said, but "the reasonable expectation of privacy can be easily extinguished" with explicit employer policies on IM use.

Digital Discovery	
& e-Evidence	
www.pf.com/digitaldisc.asp	
Managing Editor , Carol L. Eoannou	800/255-8131 ext. 269 (ceoannou@pf.com)
Legal Editor , Robert Emeritz	800/255-8131 ext. 258 (remeritz@pf.com)
News Editor , Scott Sleek	800/255-8131 ext. 291 (ssleek@pf.com)
Contributing Editor , Faith Ruderfer	800/255-8131 ext. 288 (fruderfer@pf.com)
Group Publisher , Meg Hargreaves	800/255-8131 ext. 229 (mhargreaves@pf.com)
Copy Editor , Marie Unger; Layout and Design Manager , Jennifer Andruzzi	
Published monthly, except for August. ISSN: 1537-5099	attorney. Pike & Fischer is not responsible for any claim, liability,
Subscription rate: \$549	or damage related to the use of information in <i>Digital Discovery &</i>
© Copyright ©2003 Pike & Fischer, Inc. All rights reserved.	<i>e-Evidence</i> . Also, the views expressed by outside authors do not
POSTMASTER: Send address changes to: <i>Digital Discovery</i> , Pike	necessarily represent the views of Pike & Fischer.
& Fischer, Inc., 1010 Wayne Avenue, Suite 1400, Silver Spring,	Publisher: Pike & Fischer, Inc., a subsidiary of The Bureau of
MD 20910	National Affairs, Inc., 1010 Wayne Avenue, Suite 1400, Silver
Disclaimer: Pike & Fischer, Inc., has created this publication to	Spring, MD 20910
provide you with accurate, concise and authoritative information	No reproductions may be made without prior written authorization
on developments in electronic evidence and discovery. However,	from Pike & Fischer, nor shall this information, either in whole or in
the information in this publication should not be interpreted as legal	part, be redistributed or put into a computer without the prior
advice, and should not be used as a substitute for advice from an	written permission of Pike & Fischer.

As for employers using IM to communicate with employees, and perhaps using it to verify that workers are at their stations, Sobel said employers would be wise to offer full disclosure in their IM policies, setting forth both rules on employee IM use and how the employer will use the technology.

Overly said that for the last few years, he has begun adding IM to the electronic communications policies he drafts for employer clients. He also recommends that companies send out

memos informing workers that they are prohibited from installing IM software unless the company gives specific authorization.

“Employers need to treat instant messaging the same way they treat e-mail,” Flynn said. She suggests that with both e-mail and IM, employers follow “the three Es”:

- Establish written rules and policies.
- Educate employees on usage.

- Enforce policies with disciplinary action and software.

Employers already have had to take disciplinary action against workers for improper use of company e-mail systems, Flynn said. “You’re going to see a growing number of employers who will in fact be terminating employees over inappropriate IM use,” she predicted.

“Develop an acceptable use policy and educate your employees,” Flynn advised. “The easiest way to control risk is to control content.”

Conference Report

Trial Strategy

Agreements Should Govern Experts’ Work Product Disclosure, Panelists Urge

From e-mails to electronic drafts, attorneys can agree at the beginning of a case about what records experts need to retain to reduce some disputes later in litigation, panelists at the American Bar Association Annual Meeting said Aug. 8.

Production of expert work product, draft reports and notes, and other disclosure issues are central to trial strategy, attorneys attending a session on expert witnesses were told.

“In fact, one and a half percent—maybe—of civil cases really are going to trial,” said U.S. District Judge Shira Scheindlin (S.D. N. Y.).

“The case is going to be won or lost long before trial because it’s never going to trial. It’s either going to settle or [be lost] on motions. And it seems to me that’s got to be factored into your strategy as to what you’re doing with all these experts up to the day of trial, which is never going to come,” Scheindlin said.

Early Resolution of Disclosures

Attorneys can by agreement with opposing counsel “take care of a lot of these issues. Do it early on before you hate each other,” advised Steve Saltzburg, a law professor at George Washington University.

“The idea of reasonable people saying, ‘Let’s agree on what we’re taking out of this,’ is a very attractive proposition,” he added.

Retaining E-mail and Draft Reports

Deborah Ballati, a partner with Farella, Braun & Martel in San Francisco, said she tells her experts “they have to preserve everything.”

While Ballati said she does not include in the retainer agreement that e-mails have to be preserved, she strongly encourages that practice.

Keith Ugone, a Pricewaterhouse-

Coopers partner in Dallas, said as an economist, all experts have work paper files that includes a correspondence file. “I find e-mail no different [from] correspondence. I view the e-mail the same as getting a letter. I save that no matter what,” Ugone said.

“Fortunately,” said Gregory Joseph with the Gregory Joseph Law Offices in New York, “nobody asks for voicemail because nobody’s preserved their own voicemail. There’s no principal difference between e-mail and voicemail.”

“Where the world has changed for me is the concept of drafts,” Ugone said.

Ugone estimates that in the last five cases, “I more and more just save the draft as part of my work paper.” The question becomes when to show the attorney the draft, he said.

Scheindlin said, “The problem is deletion. With paper drafts, people might have really printed it out and it’s gone. The problem with electronic data is it’s never gone. It can always be excavated.”

In the electronic world, “the prior drafts are maintained in the embedded data,” Scheindlin said.

With the very deep pockets of the U.S. government, excavations can be funded if prosecutors desire, the judge said.

More Diligent Gatekeepers?

Judges have enormous discretion, Saltzburg said. “The fact of the matter is, those of us who watch the cases have

seen more evidence excluded and summary judgments granted in recent years than we’d ever seen before. And those are only reported cases,” he said.

Scheindlin said the question is whether judges have some duty *sua sponte* to be gatekeepers. “In theory we’re supposed to be thinking all along, ‘Should this be in or should this be out?’ And I think a conscientious judge might just do that,” she said.

Talking Tech

Forensics

Do-It-Yourself Electronic Discovery Tools

By George Socha

Increasingly, I hear demands from in-house and outside personnel alike for software tools they can use themselves to work with electronic discovery. They make it clear to me that while they appreciate the need to work with service bureaus in many situations, they often have projects they want to be able to handle internally.

Following is a listing of software tools for the do-it-yourselfer. The tools range from ones intended only for use by properly trained forensics specialists to ones any of us can load on our machines and begin working with after only minimal instruction. This list is not complete, of course, and any omissions or miscategorizations are my fault and my fault alone.

Before proceeding with the list, one caveat must be noted: Let the user beware! Improper use of any of these tools can lead to trouble, potentially serious trouble. In addition, neither the publisher of *Digital Discovery and e-Evidence* nor I endorse the use of any of the tools listed below.

Computer Forensics Tools for the Seriously Serious User

- ❑ Case Agent Companion, Decryption Collection, Email Examiner, Forensic Sorter, Forensic Replicator, Network Email Examiner, PDA Seizure, and Text Searcher, from Paraben Corporation, <http://www.paraben-forensics.com/products.htm>: Various computer forensics tools.
- ❑ Encase Forensic Edition and Encase Enterprise Edition, from Guidance Software, Inc., [\[www.guidancesoftware.com\]\(http://www.guidancesoftware.com\): Used to gather and preserve forensically correct copies of computer hard drives and other storage media and then to manage and evaluate the preserved information. Allows searching of “deleted” files, file slack and unallocated space.](http://</div><div data-bbox=)

❑ Ultimate Toolkit, from AccessData Corp., <http://www.accessdata.com>: Intended for conducting forensic examinations, permits file filtering and searching. Employs Stellant’s Outside In Viewer to view various file types and dtSearch for full-text indexing. Includes password recovery capabilities.

❑ WinHex and Evidor, from X-Ways Software Technology AG, <http://www.x-ways.com>: WinHex is a universal hexadecimal editor that can be used to inspect files, recover deleted files, and carry out other computer forensics tasks. Evidor can be used to search the contents of hard drives.

Litigation Support Packages with Electronic Discovery Capabilities

❑ Concordance EX, from Dataflight Software, Inc., <http://www.dataflight.com>: Organize, search, and retrieve e-mail with attachments. Import contents of PSTs, with metadata and text formatting preserved, attachments copied locally and hyperlinked; able to pull in metadata and searchable text from PDFs; convert Office documents to RTF and import.

❑ Summation 2.5, from Summation Legal Technologies, Inc., <http://www.summation.com>: The newest version of Summation comes with a set of tools for processing e-mail and related electronic files from Microsoft Outlook PST and Lotus Notes NSF files, loading the data into Summation for use with Summation’s search and other tools, and producing all or part of that data to others.

Tools for Converting Electronic Files to Image Formats (PDF, TIFF, etc.)

- ❑ Discovery Cracker, from DocuLex, Inc., <http://www.doculex.com>: Used to capture electronic files, convert them into image files, and generate associated indexes that include full text and fielded data.
- ❑ Image Driver, from Informatik Inc., <http://www.tiffdriver.com>: Create TIFF files from printable Windows documents.
- ❑ Z-Print, from Image Capture Engineering, Inc., <http://www.imagecap.com>: A utility for batch printing or converting electronic files to TIFF image files.

Search and Processing Software

- ❑ Discovery OnDemand, from Daticon, <http://www.daticon.com>: An in-house electronic data discovery solution.
- ❑ Discovery Partner, from Electronic Evidence Discovery, Inc., <http://www.eedinc.com>: Software for reviewing and producing electronic files obtained during discovery. (See related story on page __.)
- ❑ dtSearch, from dtSearch Corp., <http://www.dtsearch.com>: Products for searching electronic files.
- ❑ eDataMatrix, from nMatrix, Inc., <http://www.nmatrix.com>: Process electronic files.
- ❑ Enfish, from Enfish Corporation, <http://www.enfish.com>: Index and search files.
- ❑ Examine32, from Aquila Software, <http://www.examine32.com>: Shareware for searching various file types and searching within ZIP archives.
- ❑ Grep, from Free Software Foundation, Inc., <http://gnu.digitaltrust.it/software/grep>: Open source software for searching files for lines containing a match to a specified pattern.
- ❑ Hard Copy Pro Plus, from Mobius Solutions, Inc., <http://www.mobiousinc.com>: Search, review and print electronic files.
- ❑ Super Text Search, from Glenn Alcott Software, <http://www.galcott.com>: A utility for searching files for text.
- ❑ Wilbur, from RedTree Development Inc., <http://wilbur.redtree.com>: Open source software for indexing and then searching files.
- ❑ Windows Grep, <http://www.wingrep.com>: A text searching tool for Windows 9x and NT.

Software for Viewing Multiple File Types

- ❑ Conversion Plus, from DataViz Inc., <http://www.dataviz.com>: Open, view, print and convert vari-

ous files types, including numerous word processing, spreadsheet, database, graphics, encoded and compressed file types; access Macintosh files from a PC.

- ❑ Quick View Plus, from Stellant, Inc., <http://www.stellent.com>: View, search and print over 225 different file types.

Software for Viewing AutoCAD Files

- ❑ Volo View Express, from Autodesk, Inc., <http://usa.autodesk.com>: Free viewer for various types of AutoCAD files.

Tools for Working with Lotus Notes, Groupwise, Other Non-Microsoft E-mail Databases

- ❑ E-Mail Shuttle, from CompuSven, Inc., <http://www.compusven.com>: Software for migrating data from one e-mail system to another.
- ❑ UniAccess, from ComAxis Technology, <http://www.comaxis.com>: Converting information from one e-mail system to another.
- ❑ Mmail.exe, from Microsoft, <http://www.microsoft.com/exchange/downloads/2000/NotesImporter.asp>: Move Lotus Notes mail databases to MS Exchange.
- ❑ Notes client, from IBM, <http://www-10.lotus.com/ldd/down.nsf>: Use copy of Notes client to work directly with Notes databases.

Screen Capture Software

- ❑ Adobe Acrobat, from Adobe Systems Incorporated, <http://www.adobe.com>: Preserve web pages as PDF files.
- ❑ Offline Explorer Pro, from MetaProducts Corporation, <http://www.metaproducts.com>: For downloading web pages.
- ❑ SnagIt, from TechSmith Corporation, <http://www.techsmith.com>: Capture screen shots as well as images, web images, text and video.
- ❑ SurfSaver, from askSam Systems, <http://www.asksam.com>: A browser add-on for saving search information found on the Web.
- ❑ WebRecord, from Canon Info. Sys. Research Australia Pty Ltd: <http://www.webrecordsw.com>: Tool for capturing and printing information from a browser.

Disk Wiping Tools

- ❑ BCWipe from Jetico, Inc., <http://www.jetico.com>: Data deletion software.
- ❑ CyberScrub, from CyberScrub LLC, <http://www.cyberscrub.com>: Data deletion software.

❑ East-Tec Eraser and East-Tec DiskSanitizer, from EAST Technologies, <http://www.east-tec.com>: Data deletion software.

❑ Eraser, from Heidi Computers Ltd., <http://www.heidi.ie/eraser>: Open-source data deletion software.

❑ WipeDrive, from AccessData Corp., <http://www.accessdata.com>: Data deletion software.

Tools for Removing Metadata

❑ ezClean, from Kraft Kennedy & Lesser: <http://www.kklssoftware.com/products/ezClean/overview.asp>: Remove metadata from Word, Excel and PowerPoint files.

❑ iScrub, from Esquire Innovations, Inc., <http://www.esquireinnovations.com>: Remove metadata from Word, Excel and PowerPoint files.

❑ Metadata Assistant, from Payne Consulting Group, Inc., <http://www.payneconsulting.com>: Remove metadata from Word and Excel files.

❑ Workshare Metawall, from Workshare Technology, <http://www.workshare.com>: Metadata removal software.

Software for Directory Listings and Comparisons

❑ Beyond Compare, from Scooter Software Inc., <http://www.scootersoftware.com>: A file and folder comparison utility.

❑ Directory Compare and Directory Printer, from Glenn Alcott Software, <http://www.galcott.com>: Compare the contents of two directories; print and expert listings of files and directories.

Password Recovery Software

❑ Passware Kit, from LostPassword.com, <http://www.lostpassword.com>: Password recovery software.

❑ Password Recovery Toolkit and Password Recovery Toolkit Professional, from AccessData Corp., <http://www.accessdata.com>: Software for recovering passwords.

Sources for Additional Miscellaneous Information

❑ FILEExt, at <http://filext.com>: A web site that will help identify file types from their extensions.

❑ Whatis.com, at <http://whatis.techtarget.com>: A web site to go to for technology-related definitions as well as an extensive listing of file extensions.

George Socha is an attorney and consultant whose business, Socha Consulting LLC, helps inform digital discovery decisions. He can be reached at 651-690-1739 or george@sochaconsulting.com.

Cases

Attorneys

Copying In-house Counsel on E-mail Doesn't Create Attorney-Client Privilege

In re: Avantel SA, 5th Cir., 2003 WL 21921109, decided August 12

The U.S. Court of Appeals for the Fifth Circuit has ordered the District Court for the Western District of Texas to reconsider its opinion that e-mails relating to a contract dispute between two telecommunications companies are not protected by attorney-client privilege and therefore must be disclosed. Although the appeals court held that the lower court used the wrong standard in accessing the confidentiality documents, it agreed with the district court that copying an attorney on a corporate e-mail is not, by itself, sufficient to invoke attorney-client privilege.

Change in Law Generates Confusion

The district court's error was applying the so-called "control-group" test to conclude that the e-mails were not privileged. The control-group test upholds the attorney-client privilege only if the individual addressing the attorney was vested by the corporation with authority both to seek legal advice and to participate significantly in the corporation's response to the advice. In 1998, however the Texas Supreme Court abandoned the control group test in favor of the "subject matter" test, for all actions arising after March of that year. Including communications of employees "made at the direction of ... superiors in the corporation" to the corporation's attorneys regarding the subject matter upon which the attorney's advice is sought, the subject matter test sweeps in a broader range of communications than the control group test. Although the disputed e-mails predated March 1998, the dispositive event for determining which

test to apply is the date the lawsuit was filed, which was September 1998. Since under the less strict “subject matter” test, the e-mails may be privileged, the case is remanded to the district court for reconsideration of its earlier order.

Copying Attorney Neither Invokes Nor Precludes Privilege

An interesting wrinkle in this otherwise straightforward fact pattern is that the disputed e-mails were not sent directly to the attorney, who was merely a “cc’d” recipient of the messages. The court of appeals asserts that merely “cc-ing” an attorney on a corporate e-mail is “clearly insufficient to establish the privilege,” noting with approval the district court’s discourse on this topic:

... [E]-mails in which in-house or outside attorneys are merely sent copies of the text of the e-mail, or in which they are merely one of many addresses, should not be privileged, unless the e-mail is directed to the attorney or sent by the attorney. ... To rule otherwise would allow parties to evade the privilege limitations by sending copies of every company-generated e-mail to the company’s attorney so as to protect the communication from discovery, regardless of whether legal services were sought or who the other recipients of the e-mail were.

The appeals court took the analysis one step further, however, reasoning that notwithstanding the fact that the attorneys were copied on the messages, the communications could still qualify for privilege under the subject matter test. Given that Texas recognizes a privilege between “representatives of the client or between the client and a representative of the client,” the status of the e-mails could not be ascertained without examining them in light of the inclusive standard set out in the subject matter test.

The Executive Summary of the Survey Report, published in August 2003, is available at <http://www.lawtechnology.org/surveys/home.html>.

Privilege

Smith & Wesson E-mail No ‘Smoking Gun,’ Due to Attorney-Client Privilege

Blumenthal v. Kimber Manufacturing, Inc., 265 Conn. 1, 826 A.2d 1088, decided July 29

An e-mail from a gun manufacturer disseminated to three fellow employees and an attorney that discussed an agreement with potentially industry-wide ramifications was a pro-

TECTED attorney-client communication not otherwise subject to disclosure under the crime-fraud exception to that privilege, according to the Connecticut Supreme Court. The ruling, made July 29, affirms the decision of the trial court.

The subject of the e-mail was an agreement entered into by the Smith & Wesson Corporation that attempted to settle actions against it brought by various governmental agencies. It required Smith & Wesson and all other signatories to adopt certain practices regarding the manufacturing, sale, and marketing of firearms. It was not popular with other gun manufacturers, none of which had signed it at the time of the proceeding before the trial court.

The state attorney general, investigating a possible retaliatory economic boycott of Smith & Wesson, initiated the discovery at issue. The attorney representing the party who sent the e-mail (who was one of the recipients) represented to the court that because the agreement arose out of a series of lawsuits that all named John Doe as a defendant, potential firearms manufacturer defendants, like Kimber, his client, needed to evaluate the agreement and the industry’s reaction to it in order to plan an effective legal strategy. He also demonstrated that the other recipients of the e-mail were senior Kimber officers. Finally, he argued that because Kimber’s legal strategy regarding these matters was in part informed by the reactions of other gun manufacturers to the agreement, it was incumbent upon Kimber’s management to track these developments and apprise him of them.

The attorney general countered that the e-mail was not privileged because it was not marked as confidential, did not request legal advice, and concerned mere ongoing business developments. Moreover, no suit was pending or threatened against Kimber. In short, argued the attorney general, respondents failed to satisfy their burden of proof to invoke the privilege, and even if they had, the e-mail would be subject to disclosure under the crime-fraud exception to the privilege, as it constituted an instrumentality in furtherance of an illegal boycott.

The Shew Test

Justice Joette Katz, writing for the panel, applied the four-prong test set forth in *Shew v. Freedom of Information Commission*, 245 Conn. 149, 714 A.2d 664 (1998) for determining whether a communication between a corporate client and an attorney is privileged: (1) the attorney must be acting in a professional capacity for the corporation, (2) the communication must be made to the attorney by current employees or officials of the corporation, (3) the communication must relate to the legal advice sought by the corporation from the attorney, and (4) the communication must be made in confidence.

The court ruled that Kimber clearly satisfied the first

prong, since the attorney-recipient was Kimber's outside counsel who represented it at both the trial and appeals levels, leading to a reasonable inference that he represented Kimber at the time the e-mail was sent. Kimber satisfied the second prong of the test with similar dispatch; the sender of the e-mail is Kimber's vice president of marketing; the party to whom it was "cc'd" is its national sales manager, and the other recipients are its president, chief financial officer, and outside counsel. All of the recipients with the exception of the attorney were Kimber employees when the e-mail was sent. The court found that their respective positions with Kimber make it evident that the recipients were members of Kimber's senior management team, which is the only showing that must be made in order to satisfy the second *Shew* criterion.

The third prong examines whether the e-mail related to legal advice sought by Kimber from the attorney recipient. The court notes that on its face, the e-mail "neither expressly requested an opinion on a legal matter, specifically raised any legal question, nor directly referred to potential litigation." However, the timing of the e-mail, within days of the announcement of the Smith & Wesson agreement, and its contents led to the reasonable inference that Kimber was anticipating similar litigation. The court observes, "[W]hen there is a credible basis to believe that ... a threat [of litigation] exists, and the client provides information to [its] attorney relating to that subject matter, the trial court can reasonably infer that the client provided the information for the

purpose of seeking legal advice." Under *Shew*, the attorney-client privilege extends to "the giving of information to the lawyer to enable counsel to give sound and informed [legal] advice." *Shew* at 157.

The fourth prong requires the communication to have been made in confidence. Noting that whether a document expressly is marked as "confidential" is but one factor a court may consider in determining confidentiality, the court agrees with the trial court's finding that the e-mail's distribution to a small number of senior managers who collectively constitute the corporate client signifies that the e-mail was intended to be confidential. The court was unpersuaded by the argument that the e-mail was merely an update on an interesting industry development; its contents go beyond a mere update, reflecting uncertainty concerning both the potential impact the agreement might have on the industry and what an appropriate response to it might be.

Accordingly, the court concludes that the trial court properly determined that the respondents had satisfied their burden of proving that the privilege insulated the e-mail from disclosure.

No Crime-Fraud Exception

The court begins from the assumption that the crime-fraud exception applies only after a determination by the trial court that there is probable cause to believe that a crime or fraud has been attempted or committed and that the com-

Is Your Professional E-mail Use Typical?

Of 3,094 lawyers surveyed in 2002 by the American Bar Association Legal Technology Resource Center:

- 80 percent send confidential or privileged communications to clients via e-mail
- 28 percent send confidential communications one or more times per day
- 23 percent send confidential communications one to four times per week
- 7 percent send confidential communications one to three times per month

The surveyed lawyers reported taking the following precautions to protect the confidentiality of client e-mail:

- 70 percent rely solely on a confidentiality statement accompanying the transmission
- 15 percent require clients to provide oral or written consent to the receipt of confidential material via e-mail
- 18 percent use encryption
- 22 percent take no precautions at all

Regarding e-mail storage:

- 93 percent of the respondents generally save incoming e-mail related to a case or client matter
- 75 percent of that group prints out hard copies of incoming e-mails
- 38 percent save the messages to a network
- 36 percent save the messages on their hard drives
- less than eight percent save e-mails onto floppy disks or other removable media

munication was in furtherance thereof. Seminal to the probable cause requirement is an inquiry whether the client's intent in seeking the legal advice was to perpetrate a crime. The petitioner failed to meet his burden of proof on this question. The court also rejects the notion that the e-mail was sent in furtherance of any crime or fraud. Its content reveals no intent to break the law, contains no words of advocacy, and refers only to the actions of others, rather than its own actions. As discussed above, it was intended to keep a corporation's outside counsel informed so that he could provide his client with sound legal advice. The court therefore concludes that the injury that would inure to the relationship of Kimber and its attorneys by disclosure of the e-mail is greater than the benefit that would be gained by its disclosure.

Attorneys

No 'Work Product' Protection for E-mail Prepared Prior to Decision to Represent

Benton v. Brookfield Properties Corp., S.D.N.Y., 2003 WL 21749602, decided July 29

Absent a prior decision to represent the insured, an internal e-mail memorandum prepared and sent by a third-party insurance company is not protected from disclosure to the estate of the plaintiff on the basis that the communication is "work product" of the defendant-insured, the U.S. District Court for the Southern District of New York ruled July 29.

Until the insurance company decides to defend the insured in a claim brought against the insured by the estates of the deceased plaintiffs, there is no relationship between the insured and the insurance company to support the "work product" privilege. The insurance company remains a "potential adversary" to the defendant-insured.

Two construction workers died in an elevator accident. Within hours of the accident, an on-site risk engineer with the insurance company prepared an initial report and e-mailed it to a senior risk manager at the insurance company's office. That manager sent a reply e-mail the following day commenting on the report and requesting certain further information. The estates of the deceased sought production of the e-mails, to which the insured objected and sought a protective order based on the premise that the e-mails constituted "work product" prepared in anticipation of litigation.

The court concluded that there was no "anticipated litigation" at the time the employee prepared his report. The employee prepared his investigation in the ordinary course of his employment with the insurance company. At the time, the employee acted solely on behalf of the insurance company. No decision had yet been made on whether the insurance company would honor the insured's claim. "[T]o qualify for work-product protection the work must have been done by or on behalf of the party, and until the insurance company decides to cover a claim, it is not a representative of the insured, but rather a potential adversary," wrote district court judge Michael H. Dolinger.

The court ordered production of the two e-mails.

Point of View

Former Police Investigators Make Top-notch Computer Forensics Experts

By Victor Limongelli,¹ John Colbert,² and Shadie Berenji³

With the vast majority of information now generated in digital format,⁴ the recovery and analysis of digital data is often a key consideration in civil litigation, as well as criminal prosecutions and internal corporate investigations. Computer forensics tools facilitate the recovery of hidden and deleted digital data, and can now do so much more efficiently and cost-effectively than ever before, even in a networked environment.

As with most tools, however, the experience and skill of the person using the tools is the most important factor leading to

ultimate success or failure. A computer forensics expert is a skilled professional who can collect, preserve, and analyze electronic evidence, and, if need be, authenticate it in court.

In the litigation context, many of the same considerations that govern the selection of any expert witness—judicial qualification as an expert and testimonial experience, for instance—will apply to the selection of a computer forensics expert, and the same legal standards concerning expert testimony will of course apply. In an internal corporate investigation, testimonial experience may not be as relevant, but other factors, such as the availability of the most up-to-date tools, may become important.

The majority of computer forensics specialists fall into one of two employment categories: those who work for law enforcement agencies, and those who work in information security roles at large corporations.⁵ Unfortunately, neither group is likely to be available to serve as an expert witness to

third parties on an ad hoc basis. These groups, however, often serve as important breeding grounds for computer forensics experts available for hire, particularly in the case of law enforcement experts, who often retire from law enforcement at a relatively young age and move into private practice.

What to Look for in Your Expert

Regardless of the context of the investigation, the following characteristics largely determine the competency of a computer forensics investigator: (1) the depth and breadth of the expert's experience; (2) the tools and techniques used by the expert; (3) the expert's organizational infrastructure; (4) the expert's ready access to additional resources within his or her organization, including the ability to conduct research quickly (particularly in novel areas); and (5) the expert's ability to communicate his or her findings both in writing and orally.

The depth and breadth of the expert's experience is important for two reasons: (1) until a computer forensics investigation is begun, it is impossible to know what types of evidence might be found on the device,⁶ thereby requiring an expert with a wide breadth of knowledge about forensic techniques and specific kinds of digital evidence; and (2) in order to qualify as a witness at trial, an expert must have sufficient "knowledge, skill, experience, training, or education"⁷ to assist the finder of fact.⁸ Indeed, for trial purposes, an expert's understanding of, and experience with, the civil litigation process (or criminal prosecutions, as the case may be) is essential.⁹

Tools and Techniques

The tools and techniques employed by the expert will often be a crucial consideration, particularly in instances in which the evidence gathered may be used in court. A court analyzing the merits of the expert's testimony determines the reliability of the principles and methodology that underlie the expert's proposed submission.¹⁰ Federal Rule of Evidence 702 sets forth the test for qualifying a witness as an expert and for ensuring that any and all scientific testimony is not only relevant, but also reliable.¹¹

In applying Rule 702 to the reliability and relevance of the expert's testimony, the trial judge must assess whether the underlying methodology utilized by the expert is scientifically valid and can properly be applied to the case.¹² The decision whether to accept an expert's testimony as scientifically valid and relevant under Rule 702 is contingent upon a determination that: (1) "the testimony is based upon sufficient facts or data; (2) the testimony is the product of reliable principles and methods; and (3) the witness has applied the principles and methods reliably to the facts of the case."¹³ In interpreting Rule 702, the Supreme Court set forth in *Daubert* the applicable test for admissibility: (1) whether

"the theory or technique in question can be (and has been) tested";¹⁴ (2) "whether it has been subjected to peer review and publications;"¹⁵ (3) "its known or potential error rate; (4) the existence and maintenance of standards controlling its

When choosing an expert, ask to see examples of reports that the expert has prepared in the past (appropriately redacted, of course) for matters similar to the one at hand. This will allow you to assess the expert's ability to communicate technical concepts and conclusions in a straightforward, understandable manner.

operations; and (5) whether it has attracted widespread acceptance within a relevant scientific community."¹⁶

Many forensic investigators still use arcane utilities, despite the availability of thoroughly tested and court-accepted commercial software. Needless to say, the more thoroughly a tool has been tested, and the wider its acceptance within the relevant community, the more likely it is to withstand a *Daubert* challenge. In addition, even outside the litigation context, if it should become necessary to replace an expert, his or her use of standard software will make the transition to a replacement expert much easier. Thus, an expert's knowledge and use of industry-standard tools is an important consideration.

Organizational Infrastructure

In addition to the qualifications of the particular individual or individuals selected to conduct the forensic investigation, the organization and environment supporting the expert will play a large role. In order to insure the admission of forensics evidence into a court proceeding, an organization conducting computer forensic examinations should have proper procedures in place (as well as formal training) for handling evidence. These should include formal documentation procedures for recording the chain of custody of all evidence, including specific release and disposal procedures. To that end, evidence should be stored in a secure facility with restricted and logged access, and all transfer of the evidence within the expert's facility should be tracked. Additionally, formal lab procedures and training should be in place to avoid cross-contamination of evidence. In this area, a law enforcement background is often invaluable for computer forensics experts, as those investigators have years of experience in observing formal evidence-handling procedures.

Research Capabilities

The expert's organizational infrastructure also comes into

play when assessing his or her ability to research specific issues quickly and thoroughly. An investigation may well present circumstances that must be intensely researched, which may include bench-testing applications. An expert should have a support structure in place to assist with such research. In addition, an expert who is part of a broader organization may well have a subordinate, peer, or supervisor with a specific expertise in the area of interest. Moreover, if the expert has in-house access to programmers, file system experts, or others with specific expertise, the expert is more likely to be able to produce fast, accurate results. When the investigator indicates that he or she never has a need for further research, then it is time to look elsewhere for an expert.

Communication Skills

Finally, the expert's ability to communicate effectively is paramount.¹⁷ "[I]t is of the utmost importance to find someone who not only knows the latest technology for examining hard drives but can communicate."¹⁸ Unfortunately, the expert may be an outstanding computer forensics expert, but may not have the ability to clearly explain the material to a jury. If an investigation is in connection with, or may lead to, litigation, then hiring an expert with testimonial experience is the best option. If testimony is likely in the case, and the expert has minimal testimonial experience, it is a good idea to talk face-to-face with the expert about technical issues. Can the expert explain those issues to you in a clear, concise manner? Or did the expert use confusing jargon and technical terms? If the expert cannot explain technical material to you, he or she is unlikely to be able to explain it to an average juror.

Written communication skills are also important. When choosing an expert, ask to see examples of reports that the expert has prepared in the past (appropriately redacted, of course) for matters similar to the one at hand. This will allow you to assess the expert's ability to communicate technical concepts and conclusions in a straightforward, understandable manner.

Law Enforcement Background

It may be difficult, especially on short notice, to find an expert who has a great deal of experience, uses industry-standard tools, has appropriate firm or organizational infrastructure to aid the investigative process, has ready access to additional resources within his or her organization, and can communicate effectively. As noted above, however, many of the individual characteristics that make for an effective computer forensics expert are developed through law enforcement training. Law enforcement forensics investigators have years of investigative experience, and usually have testified in court—and been cross-examined—on countless

occasions. A common adage in the field is, "It's much easier to teach an investigator about computers than to teach a computer expert about investigations." Law enforcement investigators have a working knowledge of legal proceedings and evidence handling procedures, as well as a clear understanding of the liabilities associated with legal matters.¹⁹ In short, law enforcement investigators typically have the requisite experience, and usually can communicate to a jury in an understandable and credible way.

Of course, you typically cannot hire an active law enforcement investigator. Retired law enforcement investigators, however, are readily available.²⁰ In choosing among them, in addition to the individual's particular qualifications, you should analyze the organizational support and infrastructure. (E.g., What tools does the organization use? Are additional resources available if needed?) The combination of an experienced, skilled former law enforcement investigator with a deep, versatile, appropriately structured organization is a winning formula for choosing a computer forensics expert.

Endnotes

¹ Victor Limongelli is general counsel of Guidance Software, Inc.

² John Colbert is senior vice president of Guidance Software, Inc., and heads its Professional Services Division.

³ Shadie Berenji is a law clerk at Guidance Software, Inc., and a third-year law student at the University of Southern California.

⁴ See *In re Bristol-Myers Squibb Securities Litigation*, 205 F.R.D. 437, 440, fn2 (2002).

⁵ Steven M. Abrams and Philip C. Weis, "Knowledge of Computer Forensics Is Becoming Essential for Attorneys in the Information Age," *New York State Bar Journal*, Feb. 2003.

⁶ Computer forensics can involve the acquisition of data from "computers, pagers, PDAs, digital cameras, cell phones, and various memory storage devices." Abrams and Philips, *supra*, note 2.

⁷ Fed. R. Evid. 702

⁸ There are also a variety of formal certifications in the computer forensics field, such as "EnCase Certified Examiner" (EnCE).

⁹ Chris Santella, "Technolawyer.com: The Growing Importance of Computer Forensics," 19 No. 13 *Law PC* 5, April 1, 2002.

¹⁰ *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 594 (1993).

¹¹ *Daubert*, 509 U.S. at 589.

¹² *Daubert*, 509 U.S. at 592.

¹³ Fed. R. Evid. 702.

¹⁴ *Daubert*, 509 U.S. at 593. *Daubert* premises the importance of this consideration on the idea that “the criterion of the scientific status of a theory is its falsifiability, or refutability, or testability.”

¹⁵ *Id.* *Daubert* further elucidates the importance of this factor by providing that “submission to the scientific community is a component of ‘good science,’ in part because it increases the likelihood that substantive flaws in the methodology will be detected.”

¹⁶ *Id.* at 594. *Daubert* is the rule in federal court and many state courts. Some states, such as California and Michigan, continue to follow the *Frye* test, which admits scientific principles or discoveries into evidence only when they were

deduced from a “sufficiently established source that has gained general acceptance in the particular field in which it belongs.” *Frye v. United States*, 293 F.1013, 1014 (1923).

¹⁷ Wade Davies, “Computer Forensics: How to Obtain and Analyze Electronic Evidence,” *Champion*, June 2003.

¹⁸ For instance, a client may request an inspection of a computer that under the conditions requested would be unlawful; a current or former law enforcement officer can warn against such action.

¹⁹ Although law enforcement investigators are normally lacking in corporate, non-criminal investigations, those who leave law enforcement and go into private practice are able to gain experience in this area as well.

Calendar

■ SEPTEMBER

16-17

LegalTech 2003. New York City. Features Litigation Technology and Electronic Data Discovery tracks. Presented by LegalTech, a division of American Lawyer Media.

Contact: Web: <http://www.legaltechshow.com>

17

Document Management and Automation for the Federal Enterprise: Improving Performance Through Innovative Business Practices (Session 3). Arlington, Va. Presented by Market*Access International, as part of its Market*Access Government Best Practices Series(tm).

Contact: Donna Anderson, tel: 703-807-2748

19-21

31st Research Conference on Communication, Information, and Internet Policy. Arlington, Va. Presented by the Telecommunications Policy Research Conference and hosted by the George Mason University Law School’s Center for Technology and Law.

Contact: tel: 301-565-3371; Internet: <http://www.tprc.org>; e-mail: info@tprc.org

22-24

National Conference on Managing Electronic Records (MER). Chicago, Ill. Presented by Cohasset Associates, Inc.

Contact: tel: 800-200-7667; Web: <http://www.cohasset.com>

25-26

2003 BNA Litigation Forum: Electronic Discovery in High-Stakes Civil Litigation. Washington, D.C. Presented by Pike & Fischer, Inc. for the Bureau of National Affairs, Inc. Key-note presentation by Magistrate Judge John Facciola, U.S. District Court for the District of Columbia.

Contact: tel: 301-562-1530; e-mail: pf@pf.com; Web: <http://www.pf.com/discovery>

■ OCTOBER

19-22

The ARMA International 48th Annual Conference and Expo. Boston, Mass.

Contact: tel: (913) 341-3808, (800) 422-2762; Web: <http://www.arma.org>

27-31

10th Conference on Computer and Communications Security. Washington, D.C. Presented by the Association of Computing Machinery.

Contact: Web: <http://www.acm.org/sigsac/ccs/CCS2003>

29-30

LegalTech 2003. Chicago, Ill. Features Litigation Technology and Electronic Data Discovery tracks. Presented by LegalTech, a division of American Lawyer Media.

Contact: Web: <http://www.legaltechshow.com>